REMARKS

Careful consideration has been given to the Official Action of February 27, 2004 and reconsideration of the application as amended is respectfully requested.

1 General Formal Matters

Pages 15, 18 and 21 are amended to overcome the examiner's objection to the drawings, by adding the reference numbers 200, 300 and 400, respectively.

The abstract has been amended by removing the reference to FIG.6.

Claims 76, 80 and 84 have been amended to delete the "such as" clauses in brackets.

Independent claims 75, 79, 83, 87, 91, 95, 99 and 103 have been amended to have consistent terminology in respect of what constitutes the 1st, 2nd, 3rd and 4th ciphertexts, the 1st and 2nd challenge signals the 1st and 2nd responses. The claims are consistent relative to each other and between the two main embodiments, described with particular reference to Figures 2 and 3.

Independent claims 75, 79, 83 and 87 have also been amended to show that they are indeed generic to both main embodiments found in the description and drawings. Nothing has been taken away from claim 75 and it is readily apparent that claim 91 can be read as being entirely within claim 75. The same goes for the other claim pairs: 79 and 95, 83 and 99 and 87 and 103. Thus claim sets 75 to 90 and 91 to 106 do indeed relate to a single invention. It is therefore respectfully submitted that all the claims presented herewith should be examined.

What actually distinguishes the two embodiments of Figures 2 and 3 of the present application from each other is the order in which certain actions occur. For the embodiment of Figure 2, the relevant order is indicated in new claims 107, 112, 116 and 120, in respect of claims 75, 79, 83 and 87 respectively. For the embodiment of Figure 3, the relevant order is indicated in claims 108, 113, 117 and 121, again in respect of claims 75, 79, 83 and 87 respectively. These claims 108, 113, 117 and 121 are generally equivalent to independent claims 91, 95, 99 and 103.

2. Comparison with the Prior Art

Overview

To date, most user authentication schemes can be classified into one of two categories, based on certain assumptions made when designing them:

i) the sharing of a known public key (e.g. Bellovin), which requires that each party knows the other party's authenticated public key; or

ii) the sharing of a secret key (e.g. Tomko), which requires that both parties share a key, such as a password.

However, the embodiments of the present invention do not belong to either category; there is no public key, nor any shared secret key. In the described embodiment, verification occurs by way of voice recognition. The independent claims are not limited to this; they merely require verification and, indeed, verification could possibly be by way of password

usage or public key use. However, the very fact that the present invention could use either distinguishes it from the prior art. Moreover, the invention is not limited to either of these and the processes of information exchange as claimed are not limited to either of these.

The present invention therefore allows two parties to set up an authenticated secure channel without being limited to either of these standard prior assumptions. Certain disadvantages that might exist as a result of such a broad approach are not present due to the arrangements of information exchange between the parties and the use of time counting, which can be used to defeat man-in-the-middle replay attacks.

In Bellovin the first step, as shown in the Figure, is to send Bob a copy of a public key. This is a well-known system and makes the authentication task straightforward. However, just because Dwork discloses the usage of time constraints in key exchange procedures, does not mean that it is necessarily obvious to incorporate such procedures into Bellovin or that it is obvious how to incorporate such procedures into Bellovin. The relevant teaching is entirely absent. Without any such teaching on how to incorporate timings, assuming one skilled in the art did decide to combine what is actually taught in the two documents (which we do not agree would happen), any combination would be no more than a random placement of time constraint use and, as such would not necessarily work.

It is not new to use time restraints to enforce security, for instance for authentication. However, the claims (both original and amended) do not lay claim to all time restraint uses. How and when to use a time restraint is not a trivial matter. In the present invention, the time restraint is a necessary part of the whole system, so as to defeat a man-in-the-middle replay

attack. On the other hand, in the Bellovin document, there are particular assumptions made about the use of a public key which is shared in advance. These assumptions are the basis of the entire proposal in this document and means that the person skilled in the art has no incentive or teaching to adapt what is disclosed to what is claimed in the present application.

In the case of Tomko, both parties have to prepare an encrypted decryption key before communication. In other words, this requires that both sides must share a password in advance. Again this makes the authentication easy. However, the key that is used is stable from use to use, thereby allowing a man-in-the-middle replay attack. On the other hand, the present invention allows users to require fresh information, for instance in the challenge signals being transmitted.

Comparison With Specific Claims

The examiner contends that all the features of claims 75, 79, 83 and 87 were known from Bellovin, except for the use of an elapsed time test. We disagree. Bellovin lacks many of the features of each independent claim.

Each of independent claims 75, 79, 91 and 95 requires the encryption and sending of two communications to a remote party, the first and fourth ciphertext, as well as the sending of g^x modulo p to the remote party. Additionally, these claims require the receiving from the remote party and decryption of two communications, the second and third ciphertexts as well as the receiving of g^y modulo p from the remote party. There are also 2 verifying steps which have nothing to do with the timing feature.

On the other hand, in Bellovin,

i.) assuming Bob is the remote party:

three communications are sent to the remote party (from the user and Alice to Bob), two encryptions and a public key, but no separate number, g^x modulo p is sent;

only one communication is received from the remote party (from Bob to Alice) and decrypted, rather than two, and no separate number, g^y modulo p is received; and

Alice generates a validation signal but carries out no validation or verification itself.

ii.) assuming Alice is the remote party:

only one communication is encrypted and sent to the remote party (from Bob to Alice), rather than two, and no separate number, g^y modulo p is sent;

three communications are received from the remote party (from the user and Alice to Bob), two encryptions and a public key, but no separate number, g^x modulo p is received; and

Alice verifies one encrypted validation signal, but only to the effect that it was sent by a party having an authentication signal and a cryptographic key K

The other independent claims, 83, 87, 99 and 103, these also require two encryptions and decryptions in each direction as well as sending a modulo number in each direction.

Likewise, they also require two verification steps on each side which have nothing to do with the timing feature. Certain of these are also lacking from Bellovin.

Going through Bellovin, we are unable to see how the examiner matches the different communications that are claimed in the present application with those shown in Bellovin. If the Examiner maintains the rejection we would be grateful for some kind of explanation.

Comparison With Specific wording

Claim 75 requires the generation of a first challenge signal. While this feature was not present in previous claim 75, it was present in previous claim 79 and therefore this feature was examined and indicated as present in Bellovin. However, it is not clear what the corresponding feature in Bellovin might be.

The first challenge signal cannot be the public key in Bellovin, because the first challenge signal is itself encrypted, while the public key is not. The first signal that is encrypted in Bellovin is the excitation signal, which is encrypted in step 113. The excitation signal, according to column 2, lines 33 to 39 is $\alpha^{RA} \text{mod} \beta$. However, claim 75 requires that the first challenge signal be of a minimum duration T which is a fixed time signal that is larger than the general transmission and processing delay. The excitation signal of Bellovin would appear not to meet this requirement.

Even if the encrypted excitation signal of Bellovin were equivalent to the first ciphertext, claim 75 also requires sending g^x modulo p to the remote party and receiving g^y

modulo p from the remote party. Neither of these is mentioned as being sent or received. g^x modulo p might possibly be regarded as a public key. However, public key delivery is beyond the scope of Bellovin. The Bellovin scheme assumes that the public key is available in advance; this further confirms that it would not be obvious to use Bellovin as a starting point in arriving at the present invention. Perhaps, the examiner considers that g^x modulo p is equivalent to the excitation signal and that in encrypting and sending the excitation signal, g^x modulo p is sent. However, this then means that the encrypted excitation signal cannot be the first ciphertext.

Claim 75 also requires the receipt of a third ciphertext. Perhaps the examiner considers this feature to be anticipated by the receipt of the encrypted response signal in Bellovin. Claim 75 also requires that a key k_b be derived from the received g^y modulo p to decrypt the second ciphertext. However, the only transfer of a relevant modulo number from Bob to Alice is the transfer of $Q = \alpha^{RB} \text{mod} \beta$, which is itself encrypted (see Bellovin, column 2, lines 49 to 55). But if this counts as the transfer of the number g^y modulo p from the remote party, then how can that itself be used to decrypt the encrypted response, that is to decrypt itself?

Claim 75 further requires that the authenticating party verify that the second challenge signal is produced by the remote party. While Alice does indeed generate a validation signal in step 127, that itself is not a verification step; verification itself only occurs in Bob in step 133.

Claim 75 further requires the authentication side to compute g^{xy} modulo p to derive a key k_{AB} and to use the key k_{AB} to decrypt the received third ciphertext. In the case of Bellovin, a key $K = Q^{RA} \text{mod} \beta$ is indeed generated, but that key is only used by Alice to generate a validation signal, not to decrypt what is received from Bob.

Claim 75 also requires that a second response of minimum duration T be produced and encrypted. While a validation signal is indeed generated at Alice, in Bellovin, there is no indication of a minimum duration.

Claim 75 also requires that the first response signal be verified to be a response produced by the remote party to the first challenge signal. Even if it is said that the excitation signal in Bellovin is equivalent to the first challenge signal and the response signal is equivalent to the first response signal (ignoring many of the other requirement of claim 75), there is still no verification of this, as claim 75 requires.

Finally, claim 75 requires use of the key k from g^{xy} modulo p for secure communication after verifying that each second challenge signal and the first response signals are produced by the remote party. Neither validation occurs in Bellovin.

Equivalent analysis can be made for each independent claim of the present application for either the Alice side or the Bob side in Bellovin. Each time, there are features required in the claim, unrelated to the use of the clock, that are lacking from Bellovin. The present claims are distinguished from what is described in Bellovin by far more then simply the use

of a clock and timing. The entire process of information exchange is completely different and there is no teaching in Bellovin or anywhere else that has been indicated that would lead one skilled in the art to the particular arrangements that are claimed.

On the matter of the use of the clock, the examiner comments that it would be obvious to one of ordinary skill in the art to modify the protocol disclosed by Bellovin to include time constraints on transmissions by each party, as disclosed by Dwork, in order to obtain zero-knowledge in concurrent executions.

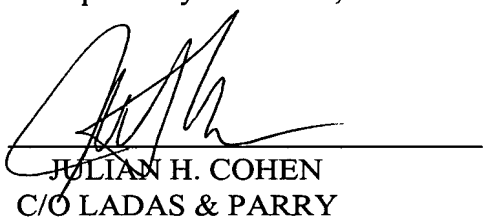
First of all, leaving aside whether the examiner's assertion is itself true, none of the claims, as such, broadly claims all zero-knowledge in concurrent executions from the transfers of information that are claimed. In each case, the clock is started and stopped at particular specific points. In the case of claim 75, g^x modulo p is sent to a remote party and the clock is started and clock is stopped after the third ciphertext is received from the remote party. Given that Bellovin does not describe the sending of a number g^x modulo p, Bellovin cannot be modified with Dwork to provide the claimed particular timing for starting the clock. Additionally, there is no equivalent of a third ciphertext in Bellovin to be received, to determine the stop timing of the clock. Even if the encrypted response signal sent from Bob to Alice were the third ciphertext, the third ciphertext that is generated by Bob, as it is described in column 2 of Bellovin, is not dependent upon the excitation signal that is sent by Alice. As such, the length of time from the sending of the encrypted excitation signal at step 113 to the receipt of the encrypted response signal in step 121, would not tell one anything about whether there is a man in the middle attack. Although there may be some use in timing

from sending the encrypted response signal in step 119 and receiving the encrypted validation signal in step 131, for Bob, there are even more differences between the present invention and the step that occur on the Bob side in Bellovin than occur on the Alice side and the present claims are distinguish by even more features.

In view of the above, it is quite clear that Bellovin is of little, if any, relevance to the present invention and that no combination of Bellovin and Dwork could lead to what is claimed.

It is therefore respectfully requested that the examiner withdraw the rejection of the claims and issue a notice of allowance in the near future.

Respectfully submitted,



JULIAN H. COHEN
C/O LADAS & PARRY
26 WEST 61ST STREET
NEW YORK, N.Y. 10023
REG. NO. 20302 - 212-708-1887